IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION AT CLEVELAND

BRADLEY OKONOSKI, individually and on behalf of all others similarly situated % DannLaw 15000 Madison Avenue Lakewood, OH 44107 Plaintiff, v. **PROGRESSIVE CASUALTY INSURANCE COMPANY** % Christina L. Crews, Law Department PO Box 5070 Cleveland, OH 44101 Defendant.	**Case No. 1:23-cv-1550** **Judge** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Bradley Okonski ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through his undersigned counsel, files this Class Action Complaint against Progressive Casualty Insurance Company ("Progressive" or "Defendant") and alleges the following based on personal knowledge of facts pertaining to him, on information and belief, and based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. This class action seeks to redress Progressive's unlawful, willful, and wanton failure to protect the highly sensitive personally identifiable information ("PII") of

approximately 347,100 individuals.[1] Due to Progressive's failure to ensure the undisclosed third-party call center[2] it hired maintained adequate data security, procedures, practices, protocols, and user controls, Plaintiff's, and the Class's PII was accessed and viewed by unauthorized actors in a massive and preventable data breach (the "Data Breach" or "Breach"), in violation of Progressive's legal obligations.[3]

2. Progressive is an insurance company based out of Mayfield Village, Ohio,[4] that provides a range of insurance products such as, personal and commercial automobile insurance, motorcycle insurance, boat insurance, property insurance, and recreational vehicle insurance.[5]

3. According to Progressive, on May 19, 2023, Progressive received written notification that some of its third-party call center's employees improperly shared their Progressive access credentials with unauthorized individuals who purportedly performed the employees' call center job duties.[6] Progressive investigated the attack with the assistance of third-party computer specialists. Thus, the unauthorized individuals had access to the personal and confidential information of some of Progressive's customers, including that of Plaintiff and the Class.[7] Progressive failed to disclose how many individuals had unauthorized access to the confidential information.

---

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/7832b375-dedf-4be0-9437-1329b9c6a55b.shtml. (last visited August 8, 2023)

[2] Hereinafter referred to as "the third-party."

[3] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/7832b375-dedf-4be0-9437-1329b9c6a55b.shtml. (last visited August 8, 2023)

[4] *See* https://www.progressive.com/locations/mayfield-village-oh-campus-1/#:~:text=Corporate%20locations%3A%20Campus%201%20in%20Mayfield%20Village%2C%20Ohio%20%7C%20Progressive. (last visited August 8, 2023)

[5] *See* https://www.progressive.com/ (last visited August 8, 2023)

[6] *See* Exhibit 1.

[7] *Id.*

4. Progressive divulged that the earliest date of employment of any of the potentially involved employees was May 2021, but most were hired during or after the fall of 2022.[8] Thus, the Breach occurred for years.

5. According to Progressive, after the Breach was discovered, it launched an investigation.[9] Based on the investigation, it determined that some of their customers' personal information may have been accessed by unauthorized individual(s).[10]

6. According to the Texas Secretary of State, the personal identifiable information exposed in the Breach included at least: names, addresses, social security numbers, driver's license numbers, and financial information (*e.g.*, account number, credit card number and/or debit card number) (the "Private Information").[11] However, what information was exposed differs from victim to victim.

7. Due to Defendant's negligence and lack of oversight and supervision of its third-party call center, unauthorized individuals obtained everything they needed to commit identity theft and fraud and wreak havoc on the financial and personal lives of hundreds of thousands of individuals.

8. In sum, Plaintiff and the Class Members have had their PII compromised as a result of (i) Progressive's inadequate data security procedures, protocols, and practices; (ii) Progressive's failure to select and utilize third-party vendors with adequate data security, procedures, practices, and protocols in place; and (iii) Progressive's failure to ensure the third-parties it hired maintained adequate data security, procedures, practices, and protocols prior to giving them access to Plaintiff's and the Class's PII. Defendant betrayed the trust of Plaintiff

[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *See* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage. (last visited August 8, 2023)

and the other Class Members by failing to properly protect and safeguard their PII, thereby enabling unauthorized individuals to view and steal their valuable and sensitive information.

9. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

10. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

Plaintiff

11. Plaintiff **Bradley Okonski** is domiciled in and a citizen of the State of Illinois. Plaintiff received a Notice of Security Incident letter ("Notice Letter") dated August 1, 2023, from Progressive informing him that his personal information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.

Defendant

12. Defendant **Progressive Casualty Insurance Company** is an Ohio corporation with its principal place of business located at 6300 Wilson Mills Road, Mayfield Village, Ohio, 44143.

III. JURISDICTION AND VENUE

13. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.[12]

14. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and upon information and belief some Class Members reside in this District.

15. Venue is likewise proper as to Defendant in this District because Defendant's principal place of business is in this District, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. The Data Breach

16. Based on information supplied by Progressive, on May 19, 2023, Progressive received written notification from its third-party call center regarding an incident involving some of its call center representatives.[13] Apparently, some of the third-party call center's employees

[12] *See* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (47,786 Texas residents impacted by the Data Breach) (last visited August 8, 2023) ; https://apps.web.maine.gov/online/aeviewer/ME/40/7832b375-dedf-4be0-9437-1329b9c6a55b.shtml (1,730 Maine residents impacted by the Data Breach) (last visited August 8, 2023).

[13] *See* Exhibit 1.

improperly shared their Progressive access credentials with unauthorized individuals, who were then able to access the Private Information of certain Progressive customers.[14]

17. Progressive did not disclose how many unauthorized actors obtained unauthorized access, but the Notice Letter indicates that it was certainly more than one unauthorized actor.[15]

18. **What is perhaps most concerning is that the Data Breach occurred for years, unnoticed and unchecked**. Progressive disclosed that the earliest date of employment of any of the potentially involved employees by the third-party call center was May 2021, however, most were hired during or after the fall of 2022.[16] Thus, unauthorized individuals had unfettered access to Plaintiff's and the Class's Private Information for more than just days or weeks, but likely years (May 2021 through May 2023).

19. Progressive gave no indication as to when the unauthorized access stopped or why it went unnoticed for so long.

20. According to disclosures made by Progressive to the Texas Attorney General, the compromised Private Information included sensitive information such as: names, addresses, social security numbers, driver's license numbers, and financial information (account numbers, credit card numbers, and/or debit card numbers).[17]

21. Despite having known about the Data Breach since May 2023, notices were not sent to affected individuals until on or around August 1, 2023 – months after the fact.

22. To make matters worse, Progressive is no stranger to inside data security threats. In 2006, a progressive employee wrongfully accessed confidential customer information,

---

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *See* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage. (last visited August 8, 2023)

including: names, Social Security numbers, dates of birth, and property addresses.[18] Clearly, Progressive was aware of the harm that could stem from insider threats, but chose to turn a blind eye. Had Progressive addressed insider threats more seriously earlier, it could have prevented this Data Breach from occurring.

23. Progressive's lax data security practices were more recently called into question again in 2015. This time, telematic devices offered by Progressive were noted to have "dozens of security flaws that could be exploited by hackers" that could cause consequences ranging from "data loss to life and limb."[19]

24. Due to Progressive's recent run of data security flaws, it is evident Progressive does not take data security seriously and does little (if anything) to protect customer data.

25. Overall, Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' Private Information from unauthorized access, including failing to supervise, monitor, and oversee all third-parties it hired who had access to Plaintiff's and the Class's PII. Progressive should have ensured any third-parties it hired had adequate data security procedures, practices, and protocols in place to eliminate unauthorized access.

---

[18] *See* https://www.computerworld.com/article/2562543/data-breach-at-progressive-highlights-insider-threat.html. (last visited August 8, 2023)

[19] *See* www.insurancebusinessmag.com/us/news/breaking-news/progressive-security-holes-put-2-million-at-risk-21007.aspx ("Telematics devices offered by Progressive Insurance, called 'Snapshot' dongles, boast dozens of security flaws that could be exploited by hackers. According to Corey Thuen, a security researcher at Digital Bond Labs, Progressive's Snapshot device is perilously insecure and vulnerable to remote cyber attacks that could be dangerous for drivers. Thuen suggested that the insurance giant does 'nothing to encrypt or otherwise protect the information [it] collects,' and as such, 'it would be possible to intercept data passed between the dongles and the insurance providers' servers.'") (last visited August 8, 2023)

26. Defendant also failed to provide timely notice to Plaintiff and Class Members of the Data Breach.

27. Defendant's actions represent a flagrant disregard of the rights of the Class Members, both as to privacy and property.

B. Plaintiff's Experience

28. Plaintiff received a Notice Letter from Progressive informing him that his personal information, including his name, address, driver's license number, email address, phone number, and date of birth were compromised in the Data Breach.[20]

29. Plaintiff's and Class Members' Private Information was entrusted to Defendant for insurance purposes with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. This included Progressive ensuring that all third-party vendors it hired employed adequate data security, procedures, protocols, practices, and appropriate user access controls.

30. Because of the Data Breach, Plaintiff's Private Information is now in the hands of criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

31. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, monitoring his accounts and personal information, reviewing his credit reports, and taking other steps in an attempt to mitigate the adverse consequences of

[20] *See* Exhibit 1.

the Data Breach. The letter Plaintiff received from Progressive specifically directed him to take these actions.[21]

32. As a direct and proximate result of the Data Breach, Plaintiff will likely need to purchase a lifetime subscription for identity theft protection and credit monitoring.

33. Plaintiff has been careful to protect and monitor his identity.

34. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of criminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Private Information; and (e) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

[21] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/7832b375-dedf-4be0-9437-1329b9c6a55b.shtml (Experian Sample Letter) (last visited August 8, 2023); *see also* Exhibit 1.

C. Criminals Have Used and Will Continue to Use Plaintiff's Private Information to Defraud Them

35. Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

36. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[22] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[23] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

37. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security

---

[22] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited August 8, 2023).

[23] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/. (last visited August 8, 2023)

> number and it's not a good idea because it is connected to your life in so many ways.[24]
>
> [Emphasis added.]

38. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[25]

39. **This was a financially motivated Breach, as the only reason the unauthorized individuals would want access to Progressive's customer's information in the first place is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein**. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[26] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[27]

40. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to Private Information, they ***will*** use it.[28]

---

[24] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited August 8, 2023).

[25] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu. (last visited August 8, 2023).

[26] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web. (last visited August 8, 2023).

[27] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/. (last visited August 8, 2023).

[28] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info. (last visited August 8, 2023).

41. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

42. For instance, with a stolen social security number, which is part of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[30]

43. The ramifications of Defendant's failure to keep Class Members' Private Information secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

44. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

45. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[31] This gives thieves ample time to seek multiple

---

[29] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu. (last visited August 8, 2023).

[30] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/. (last visited August 8, 2023).

[31] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2. (last visited August 8, 2023)

treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[32]

46. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[33]

47. Defendant's offer of limited identity monitoring to Plaintiff and the Class is woefully inadequate and will not fully protect Plaintiff from the damages and harm caused by its failures. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. Once the offered coverage has expired, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Progressive's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's Private Information)—it does not prevent identity theft.[34] Nor can an identity monitoring service remove personal information from the dark web.[35] "The people who trade in stolen personal information

---

[32] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf. (last visited August 8, 2023).

[33] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf. (last visited August 8, 2023).

[34] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html. (last visited August 8, 2023).

[35] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/. (last visited August 8, 2023).

[on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[36]

48. As a direct and proximate result of the Data Breach, Plaintiff and the Class have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

49. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;

[36] *Id.*

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves have already used that information to defraud other victims of the Data Breach;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

50. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[37] For example, Private Information can be sold at a price

[37] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/. (last visited August 8, 2023).

ranging from $40 to $200.[38] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[39]

51. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant and its third-party, is protected from further breaches by the implementation of industry standard security measures, practices, procedures, and protocols. Defendant has shown itself wholly incapable of protecting Plaintiff's Private Information – especially when considering Progressive's prior data security issues identified above.

52. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to Progressive's third-party is removed from the third-party's access.

53. Defendant acknowledged, in the Notice Letter to Plaintiff and other Class Members, that the Data Breach would cause inconvenience to effected individuals by providing numerous steps for Class Members to take in an attempt to mitigate the harm caused by the Data Breach.[40]

54. In particular, the letter acknowledged that financial harm would likely occur, advising Class Members to review and monitor their free credit reports for suspicious activity.[41]

---

[38] Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. (last visited August 8, 2023).

[39] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/. (last visited August 8, 2023).

[40] *See* Exhibit 1, attached hereto.

[41] *Id.*

55. At Progressive's suggestion, Plaintiff is desperately trying to mitigate the damage that Progressive has caused him. Given the kind of Private Information Progressive made accessible to third-parties who should have never been trusted with it to begin with, Plaintiff is very likely to incur additional damages. Because identity thieves have their Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[42]

56. None of this should have happened and it was preventable.

D. Defendant was Aware of the Risk of Cyber Attacks

57. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[43] Yahoo,[44] Marriott International,[45] Chipotle,

[42] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html. (last visited August 8, 2023).

[43] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/. (last visited August 8, 2023).

[44] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html. (last visited August 8, 2023).

[45] Patrick Nohe, *The Marriott Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/. (last visited August 8, 2023).

Chili's, Arby's,[46] and others.[47]

58. **Progressive has also personally experienced internal data security issues in recent years**.[48]

59. Progressive should certainly have been aware, and indeed was aware, that it was at risk of an internal data breach that could expose the Private Information that it collected and maintained.

60. Progressive was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

E. Progressive Could Have Prevented the Data Breach

61. Data breaches are preventable.[49] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[50] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[51]

---

[46] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b. (last visited August 8, 2023).

[47] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. (last visited August 8, 2023).

[48] *See* https://www.computerworld.com/article/2562543/data-breach-at-progressive-highlights-insider-threat.html. (last visited August 8, 2023).

[49] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012) (emphasis added).

[50] *Id.* at 17.

[51] *Id.* at 28.

62. "**Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures**. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[52]

63. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[53] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

64. Upon information and belief, Progressive failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Progressive also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program

---

[52] *Id.*

[53] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf. (last visited August 8, 2023).

(FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

65. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[54]

66. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- **Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.**
- **Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read**

[54] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view. (last visited August 8, 2023).

specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- **Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.**[55]

67. In addition, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**

  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials

- **Thoroughly investigate and remediate alerts**

  - Prioritize and treat commodity malware infections as potential full compromise;

- **Include IT Pros in security discussions**

[55] *Id.* at 3-4.

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**

  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**

  - Monitor for adversarial activities
    - Hunt for brute force attempts
    - Monitor for cleanup of Event Logs
    - Analyze logon events

- **Harden infrastructure**

  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[56]

68. Given that Defendant was storing the Confidential Information of more than 300,000 individuals, Defendant could and should have implemented all of the above measures to prevent the Data breach.

69. **Specifically, among other failures, Progressive failed to ensure that the third-party it hired maintained industry standard data security procedures, practices, and protocols.**

70. In sum, this Data Breach could have readily been prevented.

F. Defendant's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class.

[56] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/. (last visited August 8, 2023).

71. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

72. Defendant stated that it discovered the Data Breach in May 2023. And yet, Progressive did not notify affected individuals until August 2023. Even then, Progressive failed to inform Plaintiff and Class Members exactly what information was exposed, how long it was exposed, and how many individuals had unauthorized access to their Private Information in the Data Breach, leaving Plaintiff and Class Members unsure as to the scope of information that was compromised.

73. During these intervals, the criminals were exploiting the information while Progressive was secretly still investigating the Data Breach.

74. If Progressive had investigated the Data Breach more diligently and reported it sooner, Plaintiff and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

V. CLASS ACTION ALLEGATIONS

75. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

76. Plaintiff brings this action against Progressive on behalf of himself and on behalf of all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> All individuals residing in the United States who received a Notice Letter from Progressive informing them that their information may have been compromised in the Data Breach.

77. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors,

subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

78. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

79. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

80. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals affected in the Data Breach was 347,100 individuals.

81. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Progressive's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Progressive.

82. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

83. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not

impossible for members of the Class individually to effectively redress Progressive's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

84. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Private Information;

c. Whether Defendant failed to ensure the third-party vendor it hired had adequate data security, procedures, practices, and protocols.

d. Whether defendant negligently hired and/or failed to supervise the third-party it hired and gave access to Plaintiff and the Class's PII;

e. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;

f. Whether Progressive breached its duties to Plaintiff and the Class as a result of the Data Breach;

g. Whether Progressive's conduct, including its failure to act, resulted in or was the proximate cause of the breach;

h. Whether Progressive was negligent in permitting the third-party access to Plaintiff's and the Class's PII;

i. Whether Progressive was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

j. Whether Progressive failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

k. Whether Progressive continues to breach duties to Plaintiff and the Class;

l. Whether Plaintiff and the Class suffered injury as a proximate result of Progressive's negligent actions or failures to act;

m. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

n. Whether Progressive's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiffs and the Class)

85. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

86. Progressive solicited, gathered, and stored the PII of Plaintiff and Class Members, which was in turn, provided to a third-party call center.

87. Progressive had full knowledge of the sensitivity of the PII that it possessed and provided to the third-party call center and the potential harm that Plaintiff and Class Members could and would suffer if their PII were wrongfully accessed by unauthorized individuals.

88. Progressive had a duty to Plaintiff and Class Members to exercise reasonable care in selecting, monitoring, and ensuring any third-party provider it hired implemented adequate data security, procedures, and protocols to prevent foreseeable harm to Plaintiffs and the Class. Including limiting unnecessary access to Plaintiff and the Class's PII.

89. Progressive had a common law duty to exercise reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when selecting a third-party provider. Specifically, when selecting a third-party provider who was entrusted with accessing, storing, safeguarding, handling, collecting, and/or protecting the PII provided by Plaintiff and the Class. This duty included taking action to ensure that all third-party providers adequately safeguarded such data, limited unnecessary third-party user access to the Private Information of Plaintiff and the Class, and implemented industry standard security procedures, practices, and protocols. Progressive utterly failed to do any of the above.

90. Progressive was also responsible for providing timely notification of the Data Breach to Plaintiff and Class Members but failed to do so.

91. Progressive breached its duties owed to Plaintiff and the Class.

92. Plaintiff and the Class were injured as a direct and proximate result of Progressive's breaches of their duties.

93. Plaintiff and Class Members continue to suffer damages and are at an imminent risk of additional harms and damages due to Progressive's breaches.

94. Accordingly, Plaintiffs and the Class are entitled to compensatory and injunctive

relief in an amount to be set forth at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of all Plaintiffs and the Class)

95. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

96. Through the use of Plaintiff's and Class Members' Private Information, Defendant received monetary benefits.

97. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and Class Members.

98. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

99. However, acceptance of the benefit under the facts and circumstances described herein make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on a third-party with adequate data security measures, procedures and protocols to secure Plaintiff's and Class Members' Private Information. Instead of paying for a third-party who provided a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing a cheaper third-party with little to no data security measures in place. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

100. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members because

Defendant failed to ensure any third-party it hired implemented the appropriate data management and security measures.

101. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices of the third-party it retained, who had access to Plaintiff and the Class's PII.

102. If Plaintiff and Class Members knew that Defendant had given their Private Information to a third-party with virtually no data security measures in place, they would not have agreed to allow Defendant to have or maintain their Private Information.

103. As a direct and proximate result of Defendant's decision to profit rather than hire a third-party with adequate data security measures in place, Plaintiff and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably should have expended to provide a third-party with adequate data security measures to secure Plaintiff's Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of the Private Information, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

104. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

105. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of all Plaintiffs and the Class)

106. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

107. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their Private Information in order for Progressive to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' Private Information and to timely notify them in the event of a data breach.

108. Plaintiff and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

109. Plaintiff and Class Members would not have provided their Private Information to Defendant had they known that Defendant would hand it over to a third-party with no security measures in place.

110. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

111. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' Private Information by giving it to a third party with inadequate data security measures, procedures, and protocols, and by failing to provide them with timely and accurate notice of the Data Breach.

112. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of all Plaintiffs and the Class)

113. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

114. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

115. Defendant owes duties of care to Plaintiff and Class Members that require Defendant to adequately secure their Private Information and ensure it is not given to third-parties with inadequate data security measures.

116. Defendant still possesses Plaintiff's and Class Members' Private Information.

117. Defendant does not specify in the Notice Letters what steps they have taken to prevent a data breach from occurring again. Nor has it stated it terminated its relationship with the third-party.

118. Plaintiff and Class Members are at risk of harm due to the exposure of their Private Information and Defendant's failure to address the security failings that lead to such exposure.

119. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures, procedures, and protocols do not comply with its duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect

customers' personal information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

i. Monitoring all third-parties it hires.

ii. Ensuring all third-parties it hires employ industry standard data security measures, procedures, practices, and protocols.

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training their security personnel and third-parties regarding any new or modified procedures;

v. Segmenting their user applications by, among other things, creating access controls;

vi. Conducting regular database scanning and security checks;

vii. Routinely and continually conducting internal training and education to inform internal security personnel and third-parties how to identify and contain a breach when it occurs and what to do in response to a breach;

viii. Purchasing credit monitoring services for Plaintiff and Class Members for a period of ten years; and

ix. Meaningfully educating Plaintiff and Class Members about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

FIFTH CAUSE OF ACTION
NEGLIGENT TRAINING, HIRING, AND SUPERVISION
(On behalf of Plaintiff and the Class)

120. Plaintiff incorporates the foregoing paragraphs as though fully set forth herein.

121. At all relevant times, the third-party was Progressive's agent. Progressive granted the third-party access to the PII of Plaintiff and the Class without properly vetting the third-party, inquiring about/ investigating the third-party's data security, training the third-party, advising the third-party of its duties owed to Plaintiffs and the Class, and/or advising the third-party of the confidential nature of Plaintiffs' and the Class's PII.

122. Progressive was negligent and failed to exercise the requisite standard of care in the hiring, supervision, and retention of the third-party – who disclosed Plaintiffs' and the Class's PII without authorization and caused the damages delineated herein by virtue of the Data Breach.

123. At all times relevant hereto, Progressive owed a duty to Plaintiff and the Class to train and supervise its agents and third-parties handling sensitive PII in its possession to ensure they recognized the duties owed to Plaintiffs' and the Class to keep their PII safe from unauthorized access.

124. Progressive owed a duty to Plaintiff and the Class to ensure the third-party implemented adequate data security, procedures, and protocols sufficient to protect Plaintiffs' and the Class's PII from unauthorized access prior to hiring the third-party.

125. Progressive also owed a continuing duty to Plaintiff and the Class to ensure the third-party continued to employ adequate data security, procedures, and protocols sufficient to protect Plaintiffs' and the Class's PII from unauthorized access after hiring the third-party.

126. Progressive breached this duty by failing to ensure the third-party possessed the requisite data security, procedures, practices, infrastructure, and protocols to protect Plaintiffs' and the Class's PII from unauthorized access prior to hiring the third-party and while the third-party worked for Progressive.

127. Progressive was on notice of the importance of data security because of well publicized data breaches occurring throughout the United States, and the prior insider threat Progressive has already dealt with. Despite knowledge of prior data breaches and unauthorized access, Progressive failed to ensure the third-party possessed the adequate security posture to protect Plaintiffs' and the Class's PII from unauthorized disclosure.

128. Progressive knew or should have known that the failure to ensure the third-party employed adequate data security, procedures, and protocols would create an unreasonable risk of danger to persons and property.

129. As a direct and proximate result of Progressive's breach of its duties, and its negligent hiring, training, selection, and supervision, of the third-party, which resulted in the unauthorized access of Plaintiff's and Class members' confidential PII, Plaintiff and the members of the Class suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, loss of privacy, diminution in value of their PII, and actual misuse of their PII.

130. Progressive was advised of the Breach, but continues to employ the third-party, putting Plaintiff and the Class at risk of more data breaches in the future.

131. The acts and omissions of Progressive in negligently hiring, retaining, training, and/or supervising the third-party are such as to show gross negligence and reckless disregard for the safety of others and, therefore, punitive damages are appropriate.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class

counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

Respectfully submitted,

/s/: Brian D. Flick
Brian D. Flick (0081605)
Marc E. Dann (0039425)
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
(513) 645-3488
(216) 373-0536 facsimile
notices@dannlaw.com

Counsel for Plaintiff and the Putative Class